Refinement by interpretation in π-institutions

César J. Rodrigues
Dep. Informatics & CCTC,
Minho University, Portugal
cjr@di.uminho.pt

Manuel A. Martins
Dep. Mathematics,
Aveiro University, Portugal
martins@ua.pt

Alexandre Madeira
Dep. Informatics & CCTC,
Minho University, Portugal
Dep. Mathematics,
Aveiro University, Portugal
Critical Software S.A., Portugal
madeira@ua.pt

Luís S. Barbosa
Dep. Informatics & CCTC,
Minho University, Portugal
lsb@di.uminho.pt

The paper discusses the role of interpretations, understood as multifunctions that preserve and reflect logical consequence, as refinement witnesses in the general setting of π-institutions. This leads to a smooth generalization of the "refinement by interpretation" approach, recently introduced by the authors in more specific contexts. As a second, yet related contribution a basis is provided to build up a refinement calculus of structured specifications in and across arbitrary π-institutions.

1 Introduction

The expression *refinement by interpretation* was coined in [MMB09b] to refer to an alternative approach to refinement of equational specifications in which signature morphisms are replaced by *logical interpretations* as refinement witnesses.

Intuitively, an interpretation is a logic translation which preserves and reflects meaning. Actually, it is a central tool in the study of equivalent algebraic semantics (see, *e.g.*, [Wój88, BP89, BP01, BR03, Cze01]), a paradigmatic example being the interpretation of the *classical propositional calculus* into the *equational theory of boolean algebras* (cf. [BP01, Example 4.1.2]). Interestingly enough, and in the more operational setting of formal software development, the notion of interpretation proved effective to capture a number of transformations difficult to deal with in classical terms. Examples include data encapsulation and the decomposition of operations into atomic transactions [MMB09b].

A typical refinement pattern that is not easily captured by the classical approach concerns refinement of a subset of operations into operations defined over more specialized sorts. This kind of transformation induces the loss of the functional property on the operations' component of signature morphisms. For example, there is not a signature morphism σ to guide a refinement where a specification with operations $g : s' \to s$ and $f : s' \to s$ is transformed into one with operations $g : s' \to s_{new}$ and $f : s' \to s$, since this translation naturally induces a map $\sigma_{sort}(s) = \{s, s_{new}\}$ which violates the definition of signature morphism.

The approach seems also promising in the context of new, emerging computing paradigms which entail the need for more flexible approaches to what is taken as a valid transformation of specifications, as in, for example, [BSR04]. Later, in [MMB09a], the whole framework was generalized from the original equational setting to address deductive systems of arbitrary dimension. This made possible, for example, to refine sentential into equational specifications and the latter into modal ones. Moreover, the restriction to logics with finite consequence relations was dropped which resulted in increased flexibility

J. Derrick , E.A. Boiten, S. Reeves (Eds.):
Refinement Workshop 2011.
EPTCS 55, 2011, pp. 53–64, doi:10.4204/EPTCS.55.4

along the software development process. The interested reader is referred to both papers for a number of illustrative examples.

On the other hand, the notion of an institution [GB92], proposed by J. Goguen and R. Burstall in the late 1970s, has proven very successful in formalizing logical systems and their interrelations.

This paper aims at lifting the use of logic interpretations to witness refinement of specifications at an institutional level. This is made in the context of π-institutions [FS88] which deal directly with syntactic consequence relations rather than with semantical satisfaction, as in the original definition of an institution [GB92]. π-institutions are particularly useful in formalizing deductive systems with varying signatures, which are only indirectly handled by the methods of abstract algebraic logic, as in [BP01] on which our first generalization [MMB09a] is based. In general, π-institutions provide a more operational framework with no loss of expressiveness as any classical institution can be suitably translated.

Refinement by interpretation is proposed here at two different levels: a *macro* level relating different π-institutions, and the *micro* level of specifications inside a particular, although arbitrary, π-institution. The former discusses what is an interpretation of institutions and provides the envisaged generalization of this approach to refinement of arbitrary deductive systems. The latter, on the other hand, corresponds to a sort of *local* refinement witnessed by interpretations thought simply as multifunctions relating sentences generated by different signatures within the same institution.

As a second, although related, contribution, the paper lays the basis for a refinement-by-interpretation calculus of structured specifications in an arbitrary (and across) π-institution(s). That both levels can be addressed and related to each other comes to no surprise: a main outcome of institution theory is precisely to provide what [AN94] describes as *effective mechanisms to manipulate theories in an analogous way as our deductive calculi manipulate formulas*.

The remainder of this paper is organized as follows. π-institutions and a notion of interpretation between them are reviewed in section 2. Then, section 3 characterizes refinement by interpretation in this context, whereas the local view is discussed in section 4. The structure of a refinement calculus is discussed in section 5. Section 6 concludes and highlights some pointers to related work.

2 π-institutions and interpretations

In broad terms, an institution consists of an arbitrary category *Sign* of signatures together with two functors SEN and MOD that give, respectively, for each signature, a set of sentences and a category of models. For each signature, sentences and models are related via a satisfaction relation whose main axiom formalizes the popular aphorism *truth is invariant under change of notation* [Dia08]. Such a very generic way to capture a logical system was originally motivated by quite pragmatic concerns: to provide an abstract, language-independent framework for specificifying and reasoning about software systems, in response to the explosion of specification logics. Several current specification formalisms, notably, CafeOBJ [DF02], CASL [MHST03] and HETS [MML07] were designed to take advantage of such a general framework.

π-institutions, proposed by J. Fiadeiro and A. Sernadas in [FS88], fulfill a similar role, replacing semantical satisfaction by a syntactic consequence relation *à la* Tarski. Therefore, a π-institution introduces, for each signature, a closure operator on the set of its sentences capturing logical consequence. As remarked by G. Voutsadakis in [Vou03] π-institutions *may be viewed as the natural generalization of the notion of a deductive system on which a categorical theory of algebraizability, generalizing the theory of [BP01] may be based*. In the sequel we review the basic definition and adopt Voutsadakis's notion of interpretation to define refinement by interpretation in such a general setting.

Definition 1 *A π-institution I is a tuple $\langle Sign, \mathsf{SEN}, (C_\Sigma)_{\Sigma\in|Sign|}\rangle$ where*

- *Sign is a category of signatures and signature morphisms;*
- $\mathsf{SEN} : Sign \to Set$ *is a functor from the category of signatures to the category of small sets giving, for each $\Sigma \in |Sign|$, the set $\mathsf{SEN}(\Sigma)$ of Σ-sentences and mapping each $f : \Sigma_1 \to \Sigma_2$ to a* substitution *$\mathsf{SEN}(f) : \mathsf{SEN}(\Sigma_1) \to \mathsf{SEN}(\Sigma_2)$;*
- *for each $\Sigma \in |Sign|$, $C_\Sigma : \mathscr{P}(\mathsf{SEN}(\Sigma)) \to \mathscr{P}(\mathsf{SEN}(\Sigma))$ is a mapping, called* Σ-closure, *such that, for all $A, B \subseteq \mathsf{SEN}(\Sigma)$ and $\Sigma_1, \Sigma_2 \in Sign$;*
  - **(a)** $A \subseteq C_\Sigma(A)$
  - **(b)** $C_\Sigma(C_\Sigma(A)) = C_\Sigma(A)$
  - **(c)** $C_\Sigma(A) \subseteq C_\Sigma(B)$ *for* $A \subseteq B$
  - **(d)** $\mathsf{SEN}(f)(C_{\Sigma_1}(A)) \subseteq C_{\Sigma_2}(\mathsf{SEN}(f)(A))$

Note that the Σ-closure operator of a π-institution is not required to be finitary.

Definition 2 *A π-institution $I' = \langle Sign', \mathsf{SEN}', (C'_\Sigma)_{\Sigma\in|Sign'|}\rangle$ is a* sub-π-institution *of $I = \langle Sign, \mathsf{SEN}, (C_\Sigma)_{\Sigma\in|Sign|}\rangle$ if $Sign'$ is a sub-category of Sign and, for each $\Sigma \in |Sign'|$, $\mathsf{SEN}'(\Sigma) \subseteq \mathsf{SEN}(\Sigma)$ and the Σ-closure C'_Σ is the restriction of C_Σ.*

Roughly speaking, the notion of logical interpretation underlying [MMB09a] is that of [BP89]: a multifunction (i.e., a set-valued function) relating formulas which preserves and reflects logical consequence. Note that the expressive flexibility of interpretations comes precisely from their definition as multifunctions. A corresponding definition, to be used in the sequel, was proposed, in the context of π-institutions, in [Vou03]:

Definition 3 *Given two π-institutions $I = \langle Sign, \mathsf{SEN}, (C_\Sigma)_{\Sigma\in|Sign|}\rangle$ and $I' = \langle Sign', \mathsf{SEN}', (C'_\Sigma)_{\Sigma\in|Sign'|}\rangle$, a* translation *$\langle \mathsf{F}, \alpha\rangle : I \to I'$ consists of a functor $\mathsf{F} : Sign \to Sign'$ together with a natural transformation $\alpha : \mathsf{SEN} \to \mathscr{P}\,\mathsf{SEN}'\mathsf{F}$.*

A translation $\langle \mathsf{F}, \alpha\rangle : I \to I'$ is a semi-interpretation *if, for all $\Sigma \in |Sign|$, $\Phi \cup \{\phi\} \subseteq \mathsf{SEN}(\Sigma)$,*

$$\phi \in C_\Sigma(\Phi) \quad \Rightarrow \quad \alpha_\Sigma(\phi) \subseteq C'_{\mathsf{F}(\Sigma)}(\alpha_\Sigma(\Phi)) \tag{1}$$

It is an interpretation *if,*

$$\phi \in C_\Sigma(\Phi) \quad \Leftrightarrow \quad \alpha_\Sigma(\phi) \subseteq C'_{\mathsf{F}(\Sigma)}(\alpha_\Sigma(\Phi)) \tag{2}$$

Finally, we say that a translation $\langle \mathsf{F}, \alpha\rangle$ interprets a π-institution I, if there is a π-institution $I^0 = \langle Sign^0, \mathsf{SEN}^0, (C^0_\Sigma)_{\Sigma\in|Sign^0|}\rangle$ for which $\langle \mathsf{F}, \alpha\rangle$ is an interpretation.

Note that a translation depends only on the categories of signatures and the sentence functors involved, but not on the family of closure operators. A translation is a *self-translation* if F is the identity functor Id. On the other hand, it is said to be a *functional translation* if, for every $\Sigma \in |Sign|$, $\phi \in \mathsf{SEN}(\Sigma)$, $|\alpha_\Sigma(\phi)| = 1$. Additionally, it is an *identity translation,* if for every $\Sigma \in |Sign|$, $\phi \in \mathsf{SEN}(\Sigma)$,

$$\alpha_\Sigma(\phi) = \{\phi\} \tag{3}$$

3 Refining π-institutions by interpretation

In software development the process of *stepwise refinement* [ST88b] encompasses a chain of successive transformations of a specification

$$S_0 \rightsquigarrow S_1 \rightsquigarrow S_2 \rightsquigarrow \cdots \rightsquigarrow S_{n-1} \rightsquigarrow S_n$$

through which a complex design is produced by incrementally adding details and reducing under-specification. This is done step-by-step until the class of models becomes restricted to such an extent that a program can be easily manufactured. The discussion on what counts for a valid refinement step, represented by $S_i \rightsquigarrow S_j$, is precisely the starting point of this line of research.

The minimal requirement to be placed on a refinement relation, besides being a pre-order to allow stepwise construction, is preservation of logical consequence. In the framework of π-institutions this corresponds to the following definition:

Definition 4 (Syntactic refinement) *Let $I = \langle Sign, \mathsf{SEN}, (C_\Sigma)_{\Sigma\in|Sign|}\rangle$ and $I' = \langle Sign', \mathsf{SEN}', (C'_\Sigma)_{\Sigma\in|Sign'|}\rangle$ be two π-institutions. I' is a syntactic refinement of I if $Sign$ is a sub-category of $Sign'$ and, for each $\Sigma \in |Sign|$, $\mathsf{SEN}(\Sigma) \subseteq \mathsf{SEN}'(\Sigma)$ and $C_\Sigma(\Phi) \subseteq C'_\Sigma(\Phi)$ for $\Phi \subseteq \mathsf{SEN}'(\Sigma)$.*

Clearly, a π-institution is a syntactic refinement of any of its π-sub-institutions. Refinement by interpretation, on the other hand, goes a step further:

Definition 5 (Refinement by interpretation) *Consider two π-institutions $I = \langle Sign, \mathsf{SEN}, (C_\Sigma)_{\Sigma\in|Sign|}\rangle$ and $I' = \langle Sign', \mathsf{SEN}', (C'_\Sigma)_{\Sigma\in|Sign'|}\rangle$ and let $\langle \mathsf{F}, \alpha\rangle : I \longrightarrow I'$ be a translation. I' is a* refinement by interpretation *of I via $\langle \mathsf{F}, \alpha\rangle$, written as $I \rightsquigarrow_{\langle \mathsf{F},\alpha\rangle} I'$, if*

- *there is a π-institution $I^0 = \langle Sign', \mathsf{SEN}', (C^0_\Sigma)_{\Sigma\in Sign'}\rangle$ that interprets I under translation $\langle \mathsf{F}, \alpha\rangle$;*
- *for all $\Sigma \in |Sign|$, $\Phi \subseteq \mathsf{SEN}(\Sigma)$,*

$$\phi \in C_\Sigma(\Phi) \;\Rightarrow\; \alpha_\Sigma(\phi) \subseteq C'_{\mathsf{F}(\Sigma)}(\alpha_\Sigma(\Phi))$$

Clearly, a syntactic refinement is a refinement by interpretation for a self, identity, functional interpretation, with $\mathsf{F} = Id$. The following Lemma establishes an useful characterization of refinement via interpretation:

Lemma 1 *Let $I = \langle Sign, \mathsf{SEN}, (C_\Sigma)_{\Sigma\in|Sign|}\rangle$ and $I' = \langle Sign', \mathsf{SEN}', (C_\Sigma)_{\Sigma\in|Sign'|}\rangle$ be two π-institutions and $\langle \mathsf{F}, \alpha\rangle : I \longrightarrow I'$ a translation. Then, $I \rightsquigarrow_{\langle \mathsf{F},\alpha\rangle} I'$ if I' is a syntactic refinement of some interpretation of I through $\langle \mathsf{F}, \alpha\rangle$.*

Proof. Suppose I' is a syntactic refinement of an arbitrary interpretation I^0 of I along $\langle \mathsf{F}, \alpha\rangle$. Clearly the first condition in the definition of refinement by interpretation is met. For the second, let $\Sigma \in Sign$ and $\Phi \cup \{\phi\} \subseteq SEN(\Sigma)$. Assume $\phi \in C_\Sigma(\Phi)$. Then

$$\alpha_\Sigma(\phi) \subseteq C^0_{F(\Sigma)}(\alpha_\Sigma(\Phi))$$

because $\langle \mathsf{F}, \alpha\rangle$ is an interpretation. On the other hand, I' being a syntactic refinement of I^0,

$$C^0_{F(\Sigma)}(\alpha_\Sigma(\Phi)) \subseteq C'_{F(\Sigma)}(\alpha_\Sigma(\Phi))$$

Thus, $\alpha_\Sigma(\phi) \subseteq C'_{F(\Sigma)}(\alpha_\Sigma(\Phi))$.
□

Definition 5 subsumes the corresponding notion introduced in [MMB09a] for k-dimensional deductive systems, because every k-dimensional deductive system $\langle \mathscr{L}, \vdash_{\mathscr{L}}\rangle$ over a countable set of variables V, gives rise to a specific π-institution $I_{\mathscr{L}} = \langle Sign_{\mathscr{L}}, Sen_{\mathscr{L}}, (C_{\mathscr{L}_\Sigma})_{\Sigma\in|Sign_{\mathscr{L}}|}\rangle$, built in [Vou02] as follows:

(i) $Sign_{\mathscr{L}}$ is the one-object category with object V. The identity morphism is the inclusion $i_V : V \to Fm_{\mathscr{L}}(V)$, where $Fm_{\mathscr{L}}(V)$ denotes the set of formulas constructed by recursion using variables in V and connectives in $\mathscr{L}$ in the usual way. Composition $g \cdot f$ is defined by $g \cdot f = g^\star f$, where $g^\star : Fm_{\mathscr{L}}(V) \to Fm_{\mathscr{L}}(V)$ denotes the substitution uniquely extending g to $Fm_{\mathscr{L}}(V)$.

(ii) $\mathsf{SEN}_{\mathscr{L}} : Sign_{\mathscr{S}} \to Set$ maps V to $Fm^k_{\mathscr{L}}(V)$ and $f : V \to V$ to $Fm_{\mathscr{L}}(V)$ $(f^\star)^k : Fm^k_{\mathscr{L}}(V) \to Fm^k_{\mathscr{L}}(V)$. It is easy to see that $\mathsf{SEN}_{\mathscr{S}}$ is indeed a functor.

(iii) Finally, $C_{\mathscr{L}}$ is the standard closure operator $C_V : \mathscr{P}(Fm_{\mathscr{L}}(V)) \to \mathscr{P}(Fm_{\mathscr{L}}(V))$ associated with $\langle \mathscr{L}, \vdash_{\mathscr{L}} \rangle$, i.e., $C_V(\Phi) = \{\phi \in Fm^k_{\mathscr{L}}(V) : \Phi \vdash_{\mathscr{S}} \phi\}$ for all $\Phi \subseteq Fm^k_{\mathscr{L}}(V)$.

Example 1 *The π-institution of modal logic $S5^G$ forms a (syntactic) refinement of the one for classical propositional calculus (CPC). Actually, consider the modal signature $\Sigma = \{\to, \wedge, \vee, \neg, \top, \bot, \Box\}$. Modal logic K is defined as an extension of CPC by adding the axiom $\Box(p \to q) \to (\Box p \to \Box q)$ and the inference rule $\frac{p}{\Box p}$. Logic $S5^G$, on the other hand, enriches the signature of K with the symbol $\Diamond$, and K itself with the axioms $\Box p \to p$, $\Box p \to \Box\Box p$ and $\Diamond p \to \Box\Diamond p$, cf. [BP01]. Hence, since the signature of both systems contains the signature of CPC and their presentations extend that of CPC with extra axioms and inference rules, we have CPC $\rightsquigarrow$ K and CPC $\rightsquigarrow$ $S5^G$ (actually, CPC $\rightsquigarrow$ K $\rightsquigarrow$ $S5^G$). Hence, through these refinements, one may capture more complex, modally expressed requirements introduced along the refinement process.*

Given an interpretation $\tau : Fm_{\mathscr{L}}(V) \longrightarrow \mathscr{P}(Fm_{\mathscr{L}'}(V'))$ between two deductive systems $\langle \mathscr{L}, \vdash_{\mathscr{L}} \rangle$ and $\langle \mathscr{L}', \vdash_{\mathscr{L}'} \rangle$, let us define $\langle \mathsf{F}_\tau, \tau \rangle$ as the translation between π-institutions $I_{\mathscr{L}}$ and $I_{\mathscr{L}'}$, where F_τ is a functor between single object categories, mapping, at the object level, V to V'. As expected,

Lemma 2 *An l-deductive system $\langle \mathscr{L}', \vdash_{\mathscr{L}'} \rangle$ is an interpretation of a k-deductive system $\langle \mathscr{L}, \vdash_{\mathscr{L}} \rangle$ through an interpretation τ, iff $\langle F_\tau, \tau \rangle$ interprets the π-institution $I_{\mathscr{L}}$ in $I_{\mathscr{L}'}$.*

Proof. Assume $\langle \mathscr{L}, \vdash_{\mathscr{L}} \rangle$ (respectively, $\langle \mathscr{L}', \vdash_{\mathscr{L}'} \rangle$) are defined over a countable set of variables V (respectively, V'). Being an interpretation between deductive systems, τ is a multifunction $\tau : Fm_{\mathscr{L}}(V) \longrightarrow \mathscr{P}(Fm_{\mathscr{L}'}(V'))$ such that, for all $\Gamma \cup \{\phi\} \subseteq Fm_{\mathscr{L}}(V)$,

$$\Gamma \vdash_{\mathscr{L}} \phi \;\; \Leftrightarrow \;\; \tau(\Gamma) \vdash_{\mathscr{L}'} \tau(\phi) \tag{4}$$

According to the construction of $I_{\mathscr{L}}$, detailed above, this is equivalent to

$$\phi \in C_V(\Gamma) \;\; \Leftrightarrow \;\; \tau(\phi) \subseteq C_{V'}(\tau(\Gamma)) \tag{5}$$

□

Hence, it is immediate to check that

Corollary 1 *An l-deductive system $\langle \mathscr{L}', \vdash_{\mathscr{L}'} \rangle$ is a refinement of a k-deductive system $\langle \mathscr{L}, \vdash_{\mathscr{L}} \rangle$ through an interpretation τ, iff the π-institution $I_{\mathscr{L}'}$ is a refinement of $I_{\mathscr{L}}$ through $\langle F_\tau, \tau \rangle$.*

As a final remark, note that, in a very precise sense, Definition 5 also covers the case of classical institutions. Actually, a π-institution corresponding to a classical one can always be defined: for each signature Σ and set of formulas Ψ, take $C_\Sigma(\Psi)$ as the set of sentences satisfied in all models validating Ψ.

4 The local view

Having discussed refinement by interpretation of π-institutions, we address now the same sort of refinement applied to specifications inside an arbitrary π-institution. Such is the *local* view. Given an arbitrary π-institution $I = \langle Sign, \mathsf{SEN}, (C_\Sigma)_{\Sigma \in |Sign|} \rangle$, a basic, or *flat* specification is defined as

$$SP \;=\; \langle \Sigma, \Phi \rangle$$

where $\Sigma \in |Sign|$ and $\Phi \subseteq \mathsf{SEN}(\Sigma)$. Its meaning is the closure of Φ, i.e., $C_\Sigma(\Phi)$. D. Sannella and A. Tarlecki in [ST88a] define specification over an arbitrary institution along similar lines, but taking, as semantic domain, classes of models instead of logical consequence relations.

As expected, any morphism $\sigma : \Sigma \longrightarrow \Sigma'$ in *Sign* entails a notion of *local* refinement $\rightsquigarrow_\sigma$ in I given by

$$\langle \Sigma, \Phi \rangle \rightsquigarrow_\sigma \langle \Sigma', \Phi' \rangle \;\text{ if }\; \sigma(\Phi) \subseteq C_{\Sigma'}(\Phi') \tag{6}$$

For σ an inclusion, this may be regarded as a form of syntactic refinement.

Specifications may also be connected by interpretations which, again, correspond to multifunctions preserving and reflecting consequence. Formally,

Definition 6 *Let $\langle \Sigma, \Phi \rangle$ and $\langle \Sigma', \Phi' \rangle$ be two specifications over a π-institution $I = \langle Sign, \mathsf{SEN}, (C_\Sigma)_{\Sigma \in |Sign|} \rangle$ and $i : \mathsf{SEN}(\Sigma) \longrightarrow \mathscr{P}(\mathsf{SEN}(\Sigma'))$ a multifunction from $\mathsf{SEN}(\Sigma)$ to $\mathsf{SEN}(\Sigma')$. Then i is a* (local) semi-interpretation *of $\langle \Sigma, \Phi \rangle$ in $\langle \Sigma', \Phi' \rangle$ if, for all $\phi \in \mathsf{SEN}(\Sigma)$,*

$$\phi \in C_\Sigma(\Phi) \;\Rightarrow\; i(\phi) \subseteq C_{\Sigma'}(\Phi') \tag{7}$$

It is a (local) interpretation *of $\langle \Sigma, \Phi \rangle$ in $\langle \Sigma', \Phi' \rangle$ if,*

$$\phi \in C_\Sigma(\Phi) \;\Leftrightarrow\; i(\phi) \subseteq C_{\Sigma'}(\Phi') \tag{8}$$

Finally, we say that i (locally) interprets *$\langle \Sigma, \Phi \rangle$, if there is a specification $\langle \Sigma^0, \Phi^0 \rangle$ on which $\langle \Sigma, \Phi \rangle$ is interpreted by i.*

Adopting expression "*ϕ is true in* specification $\langle \Sigma, \Phi \rangle$" to abbreviate the fact that $\phi \in C_\Sigma(\Phi)$, definition (8) can be read as *ϕ is true in $\langle \Sigma, \Phi \rangle$ iff $i(\phi)$ is true in $\langle \Sigma', \Phi' \rangle$*.

Definition 7 *Let $SP = \langle \Sigma, \Phi \rangle$ be a specification and $i : \mathsf{SEN}(\Sigma) \longrightarrow \mathscr{P}(\mathsf{SEN}(\Sigma'))$ a translation which interprets SP. A specification $SP' = \langle \Sigma', \Phi' \rangle$ refines SP via local interpretation i, written as $SP \rightsquigarrow_i SP'$, if for all $\phi \in \mathsf{SEN}(\Sigma)$,*

$$\phi \in C_\Sigma(\Phi) \;\Rightarrow\; i(\phi) \subseteq C_{\Sigma'}(\Phi') \tag{9}$$

Given a $\sigma : \Sigma \to \Sigma' \in Sign$, $\mathsf{SEN}(\sigma) : \mathsf{SEN}(\Sigma) \to \mathsf{SEN}(\Sigma')$ induces a translation that maps each $\phi \in \mathsf{SEN}(\Sigma)$ into $\{\mathsf{SEN}(\sigma)(\phi)\}$. In the sequel we identify this translation simply with $\mathsf{SEN}(\sigma)$.

Definition 8 *A signature morphism $\sigma : \Sigma \to \Sigma' \in Sign$ is* conservative *if for any $\Phi \subseteq \mathsf{SEN}(\Sigma)$, $\mathsf{SEN}(\sigma)$ interprets $\langle \Sigma, \Phi \rangle$ in $SP^\sigma = \langle \Sigma', \mathsf{SEN}(\sigma)(\Phi) \rangle$.*

Observe that $\mathsf{SEN}(\sigma)$ is always a semi-interpretation from SP to SP^σ. Moreover, note that conservativeness is a stronger notion than that of interpretability.

Theorem 1 *Let $\sigma : \Sigma \to \Sigma' \in Sign$ be a conservative signature morphism, $SP = \langle \Sigma, \Phi \rangle$ a specification over I and $\Phi' \in \mathsf{SEN}(\Sigma')$. Then,*

$$\mathsf{SEN}(\sigma)(\Phi) \subseteq C_{\Sigma'}(\Phi') \text{ implies that } SP \rightsquigarrow_{\mathsf{SEN}(\sigma)} \langle \Sigma', \Phi' \rangle \tag{10}$$

In practice, new specifications are built from old through application of a number of specification constructors. As a minimum set we consider operators to join two specifications, to translate one into another, and to derive one from another going backward along a signature morphism. The following definition characterizes along these lines a notion of structured specification in an arbitrary π-institution.

Definition 9 *Structured specifications over an arbitrary π-institution $I = \langle Sign, \mathsf{SEN}, (C_\Sigma)_{\Sigma \in |Sign|} \rangle$ are defined inductively as follows, taking flat specifications as the base case.*

- *For a signature Σ, the union of specifications $SP_1 = \langle \Sigma, \Phi_1 \rangle$ and $SP_2 = \langle \Sigma, \Phi_2 \rangle$ is defined as*

$$\mathsf{union}(SP_1, SP_2) \;=\; \langle \Sigma, \Phi_1 \cup \Phi_2 \rangle$$

- *The translation of specification $SP = \langle \Sigma, \Phi \rangle$ through a morphism $\sigma : \Sigma \to \Sigma'$ in Sign is defined as*

$$\mathsf{translate}\ SP\ \mathsf{through}\ \sigma \;=\; \langle \Sigma', \mathsf{SEN}(\sigma)(\Phi) \rangle$$

- *The derivation of a Σ specification from $SP' = \langle \Sigma', \Phi' \rangle$ through a morphism $\sigma : \Sigma \to \Sigma'$ in Sign is defined as*

$$\mathsf{derive}\ SP'\ \mathsf{through}\ \sigma \;=\; \langle \Sigma, \Psi \rangle$$

where $\Psi = \{\psi |\ \mathsf{SEN}(\sigma)(\psi) \in C_{\Sigma'}(\Phi')\}$.

Of course, it is desirable that refinement be preserved by horizontal composition of specifications. In particular, refinement by interpretation should be preserved by all specification constructors in Definition 9. The result is non trivial. For union we have,

Lemma 3 *Let $i : \mathsf{SEN}(\Sigma) \longrightarrow \mathscr{P}(\mathsf{SEN}(\Sigma'))$ be a local interpretation, and $SP_1 = \langle \Sigma, \Phi_1 \rangle$, $SP_2 = \langle \Sigma, \Phi_2 \rangle$ specifications such that $SP_1 \rightsquigarrow_i SP_1'$ and $SP_2 \rightsquigarrow_i SP_2'$. If i interprets $\mathsf{union}(SP_1, SP_2)$, then $\mathsf{union}(SP_1, SP_2) \rightsquigarrow_i \mathsf{union}(SP_1', SP_2')$.*

Proof. For all $\phi \in \mathsf{SEN}(\Sigma)$, we reason

$$\begin{array}{ll}
 & SP_1 \rightsquigarrow_i SP_1' \ \wedge\ SP_2 \rightsquigarrow_i SP_2' \\
\Leftrightarrow & \quad \{\text{ definition}\} \\
 & \phi \in C_\Sigma(\Phi_1) \Rightarrow i(\phi) \subseteq C_{\Sigma'}(\Phi_1') \ \wedge\ \phi \in C_\Sigma(\Phi_2) \Rightarrow i(\phi) \subseteq C_{\Sigma'}(\Phi_2') \\
\Rightarrow & \quad \{\, C_\Sigma, C_{\Sigma'} \text{ monotonic}\} \\
 & \phi \in (C_\Sigma(\Phi_1) \cup C_\Sigma(\Phi_2)) \Rightarrow i(\phi) \subseteq (C_{\Sigma'}(\Phi_1') \cup C_{\Sigma'}(\Phi_2')) \\
\Leftrightarrow & \quad \{\text{ definition}\} \\
 & \mathsf{union}(SP_1, SP_2) \rightsquigarrow_i \mathsf{union}(SP_1', SP_2')
\end{array}$$

□

The remaining cases are not straightforward. Actually, achieving compatibility entails the need for imposing some non trivial conditions on morphisms.

5 Towards a refinement calculus

Having defined refinement by interpretation *across* π-institutions and *inside* an arbitrary π-institution, this section sketches their interconnections. Our first step is to define how a specification in an institution I translates to I' along an interpretation.

Definition 10 *Let $\rho = \langle \mathsf{F}, \alpha \rangle : I \longrightarrow I'$ be a translation between π-institutions I and I' and $SP = \langle \Sigma, \Phi \rangle$ a specification in I. The translation $\hat{\rho}(SP)$ of SP through ρ is defined by*

$$\hat{\rho}\,\langle \Sigma, \Phi \rangle \;=\; \langle \mathsf{F}(\Sigma), \alpha_\Sigma(\Phi) \rangle \tag{11}$$

Next lemma answers the following question: is refinement by interpretation over arbitrary π-institutions preserved by the specification constructors?

Lemma 4 *The definition of specification translation is structural over the specification constructors given in definition 9, i.e.*

$$\begin{aligned}
\hat{\rho}\,(\mathsf{union}(SP_1, SP_2)) &= \mathsf{union}(\hat{\rho}(SP_1), \hat{\rho}(SP_2)) \\
\hat{\rho}\,(\mathsf{translate}\ SP\ \mathsf{through}\ \sigma) &= \mathsf{translate}\ \hat{\rho}(SP)\ \mathsf{through}\ \mathsf{F}(\sigma) \\
\hat{\rho}\,(\mathsf{derive}\ SP'\ \mathsf{through}\ \sigma) &= \mathsf{derive}\ \hat{\rho}(SP')\ \mathsf{through}\ \mathsf{F}(\sigma)
\end{aligned}$$

Proof. For the first case let $SP_1 = \langle \Sigma_1, \Phi_1 \rangle$ and $SP_2 = \langle \Sigma_2, \Phi_2 \rangle$. Then,

$$\begin{aligned}
& \hat{\rho}\,(\mathsf{union}(SP_1, SP_2)) \\
= & \qquad \{ \text{ definition of } \mathsf{union} \} \\
& \hat{\rho}\,\langle \Sigma, \Phi_1 \cup \Phi_2 \rangle \\
= & \qquad \{ \text{ definition of } \hat{\rho} \} \\
& \langle \mathsf{F}(\Sigma), \alpha(\Phi_1 \cup \Phi_2) \rangle \\
= & \qquad \{ \ \alpha \text{ is a natural transformation} \} \\
& \langle \mathsf{F}(\Sigma), \alpha(\Phi_1) \cup \alpha(\Phi_2) \rangle \\
= & \qquad \{ \text{ definition of } \mathsf{union} \} \\
& \mathsf{union}(\langle \mathsf{F}(\Sigma), \alpha(\Phi_1) \rangle, \langle \mathsf{F}(\Sigma), \alpha(\Phi_2) \rangle) \\
= & \qquad \{ \text{ definition of } \hat{\rho} \} \\
& \mathsf{union}(\hat{\rho}(SP_1), \hat{\rho}(SP_2))
\end{aligned}$$

Consider now the second case (the third being similar):

$$
\begin{array}{ll}
 & \hat{\rho}\,(\mathsf{translate}\ SP\ \mathsf{through}\ \sigma) \\
= & \qquad \{\ \text{definition of } \mathsf{translate}\} \\
 & \hat{\rho}\,\langle \Sigma', \sigma(\Phi)\rangle \\
= & \qquad \{\ \text{definition of } \hat{\rho}\} \\
 & \langle \mathsf{F}(\Sigma'), \alpha_{\Sigma'}(\sigma(\Phi))\rangle \\
= & \qquad \{\ \alpha \text{ is a natural transformation}\} \\
 & \langle \mathsf{F}(\Sigma'), \mathscr{P}(\sigma)(\alpha_{\Sigma}(\Phi))\rangle \\
= & \qquad \{\ \text{definition of } \mathsf{translate}\} \\
 & \mathsf{translate}\ \langle \mathsf{F}(\Sigma'), \alpha_{\Sigma}(\Phi)\rangle\ \mathsf{through}\ \mathsf{F}(\sigma) \\
= & \qquad \{\ \text{definition of } \hat{\rho}\} \\
 & \mathsf{translate}\ \hat{\rho}(SP)\ \mathsf{through}\ \mathsf{F}(\sigma)
\end{array}
$$

Note a slight abuse of notation: the extension of $\hat{\rho}(SP)$ in the conclusion is actually through the powerset extension of $\mathsf{F}(\sigma)$.
□

6 Conclusions and related work

In software development, one often has to resort to a number of different logical systems to capture contrasting aspects of systems' requirements and programming paradigms. This paper uses π-institutions to formalize arbitrary logical systems and lifts to such level a recently proposed [MMB09b, MMB09a] approach to refinement based on logical interpretation.

Refinement by interpretation is formulated at both a global (*i.e.*, across π-institutions) and local (*i.e.*, between specifications inside an arbitrary π-institution) level. The paper introduces a notion of structured specification and shows that, at both levels, refinement by interpretation respects the proposed specification constructors. Actually, the institutional setting not only makes it possible to go a step further from [MMB09a] in generalizing the concept to arbitrary logics, but also provides a basis to build up a refinement calculus of "institution-independent", structured specifications.

We close the paper with a few remarks on *refinement by interpretation* in itself and some pointers to related work.

The idea of relaxing what counts as a valid refinement of an algebraic specification, by replacing *signature morphisms* by *logic interpretations* is, to the best of our knowledge, new. The piece of research initiated with [MMB09b] up to the present paper was directly inspired by the second and third author's work on algebraic logic as reported, respectively, in [Mar06] and [Mad08], where the notion of an *interpretation* plays a fundamental role (see, *e.g.*, [BP89, BP01, BR03, Cze01]) and occurs in different variants. In particular, the notion of *conservative translation* intensively studied by Feitosa and Ottaviano [FD01] is the closest to our own approach.

Refinement by interpretation should also be related to the extensive work of Maibaum, Sadler and Veloso in the 70's and the 80's, as documented, for example, in [MSV84, MVS85]. The authors resort

to interpretations between theories and conservative extensions to define a syntactic notion of refinement according to which a specification SP' refines a specification SP if there is an interpretation of SP' into a conservative extension of SP. It is shown that these refinements can be vertically composed, therefore entailing stepwise development. This notion is, however, somehow restrictive since it requires all maps to be conservative, whereas in program development it is usually enough to guarantee that requirements are preserved by the underlying translation. Moreover, in that approach the interpretation edge of a refinement diagram needs to satisfy a number of extra properties.

Related work also appears in [FM93, Vou05] where interpretations between theories are studied, as in the present paper, in the abstract framework of π-institutions. The first reference is a generalization of the work of Maibaum and his collaborators, whereas the second generalizes to π-institutions the abstract algebraic logic treatment of algebraic semantics on sentential logics. Notions of interpretation between institutions also appear in [Bor02] and [Tar95] under the designation of *institution representation*. Differently from the one used in this paper, borrowed from [Vou03], they are not defined as multifunctions. The work of José Meseguer [Mes89] on *general logics*, where a theory of interpretations between logical systems is developed, should also be mentioned.

We believe this approach to refinement through logical interpretation has a real application potential, namely to deal with specifications spanning through different specification logics. Particularly deserving to be considered, but still requiring further investigation, are observational logic [BHK03], hidden logic [Roş00, MP07] and behavioral logic [Hen97]. As remarked above, the study of refinement preservation by horizontal composition remains a challenge and a topic of current research.

Other research topics arise concerns the ways in which *global* and *local* levels interrelate. For example, we are still studying to what extent a local refinement by interpretation of a specification in a π-institution I, lifts to another local refinement of its translation induced by a global interpretation from I to another π-institution I'.

Acknowledgments

This research was partially supported by Fct (the Portuguese Foundation for Science and Technology) under contract `PTDC/EIA-CCO/108302/2008` — the MONDRIAN project, and the CIDMA research center. M. A. Martins was further supported by project *Nociones de Completud*, reference FFI2009-09345 (MICINN - Spain). Finally, A. Madeira was also supported by SFRH/BDE/ 33650/2009, a joint PhD grant by FCT and Critical Software S.A., Portugal.

References

[AN94] H. Andreka & I. Nemeti (1994): *General Algebraic Logic: A Perspective on "What is logic?"* In: *What is a Logical System? - Studies in Logic and Computation, Vol. 4*, Oxford University Press.

[BHK03] M. Bidoit, R. Hennicker & A. Kurz (2003): *Observational logic, constructor-based logic, and their duality. Theor. Comput. Sci.* 298(3), pp. 471–510, doi:10.1016/S0304-3975(02)00865-4.

[Bor02] T. Borzyszkowski (2002): *Logical Systems for Stuctured Specifications*. *Theor. Comp. Science* 286, pp. 197–245, doi:10.1016/S0304-3975(01)00317-6.

[BP89] W. Blok & D. Pigozzi (1989): *Algebraizable Logics*. *Memoirs of the American Mathmatical Society* 396. AMS - American Math. Soc., Providence.

[BP01] W. Blok & D. Pigozzi (2001): *Abstract Algebraic Logic and the Deduction Theorem*. Preprint available from `www.math.iastate.edu/dpigozzi/papers/aaldedth.pdf`.

[BR03] W. Blok & J. Rebagliato (2003): *Algebraic Semantics for Deductive Systems*. *Studia Logica* 74(1-2), pp. 153–180, doi:10.1023/A:1024626023417.

[BSR04] D. Batory, J. N. Sarvela & A. Rauschmayer (2004): *Scaling step-wise refinement*. *IEEE Trans. in Sofware Engineering* 30(6), pp. 355–371, doi:10.1109/TSE.2004.23.

[Cze01] J. Czelakowski (2001): *Protoalgebraic Logics*. Trends in logic, Studia Logica Library, Kluwer Academic Publishers.

[DF02] R. Diaconescu & K. Futatsugi (2002): *Logical foundations of CafeOBJ*. *Theor. Comput. Sci.* 285(2), pp. 289–318, doi:10.1016/S0304-3975(01)00361-9.

[Dia08] R. Diaconescu (2008): *Institution-independent Model Theory*. Birkhäuser Basel, doi:10.1007/978-3-7643-8708-2_2.

[FD01] H. A. Feitosa & I. M. L. D'Ottaviano (2001): *Conservative translations*. *Ann. Pure Appl. Logic* 108(1-3), pp. 205–227, doi:10.1016/S0168-0072(00)00046-4.

[FM93] J. Fiadeiro & T. S. E. Maibaum (1993): *Generalising Interpretations between Theories in the context of (pi-) Institutions*. In: *Proceedings of the First Imperial College Department of Computing Workshop on Theory and Formal Methods*, Springer-Verlag, London, UK, pp. 126–147. Available at `http://portal.acm.org/citation.cfm?id=647322.721361`.

[FS88] J. Fiadeiro & A. Sernadas (1988): *Structuring Theories on Consequence*. In D. Sanella & A. Tarlecki, editors: *Recent Trends in Data Type Specification. Specification of Abstract Data Types (Papers from the Fifth Workshop on Specification of Abstract Datac Types, Gullane, 1987)*, *Lecture Notes in Computer Science* 332, Springer-Verlag, Berlin.

[GB92] J. Goguen & R. Burstall (1992): *Institutions: abstract model theory for specification and programming*. *J. ACM* 39(1), pp. 95–146, doi:10.1145/147508.147524.

[Hen97] R. Hennicker (1997): *Structural specifications with behavioural operators: semantics, proof methods and applications*. Habilitationsschrift.

[Mad08] Alexandre Madeira (2008): *Observational Refinement Process*. *Electr. Notes Theor. Comput. Sci.* 214, pp. 103–129, doi:10.1016/j.entcs.2008.06.006.

[Mar06] Manuel A. Martins (2006): *Behavioral Institutions and Refinements in Generalized Hidden Logics*. *J. UCS - Journ. of Universal Computer Science* 12(8), pp. 1020–1049, doi:10.3217/jucs-012-08-1020. Available at `http://www.jucs.org/jucs_12_8/behavioral_institutions_and_refinements`.

[Mes89] J. Meseguer (1989): *General Logics*. In J. Bairwise & H.J. Keisler et all, editors: *Logic Colloquium'87*, 87, Elsevier, pp. 275–330.

[MHST03] T. Mossakowski, A. Haxthausen, D. Sannella & A. Tarlecki (2003): *CASL: The Common Algebraic Specification Language: Semantics and Proof Theory*. *Computing and Informatics* 22, pp. 285–321, doi:10.1.1.10.2965.

[MMB09a] M.A. Martins, A. Madeira & L.S. Barbosa (2009): *Refinement by Interpretation in a General Setting*. In E. Boiten J. Derrick & S. Reeves, editors: *Proc. Refinement Workshop 2009*, ENTCS, Elsevier, pp. 105–121, doi:10.1016/j.entcs.2009.12.020.

[MMB09b] M.A. Martins, A. Madeira & L.S. Barbosa (2009): *Refinement via Interpretation*. In: *7th IEEE International Conf. on Software Engineeering and Formal Methods, Hanoi, Vietnam*, IEEE Computer Society Press, doi:10.1109SEFM.2009.35.

[MML07] T. Mossakowski, C. Maeder & K. Lüttich (2007): *The heterogeneous tool set, HETS*. In: *13th Int. Conf. Tools and algorithms for the construction and analysis of systems*, TACAS'07, Springer-Verlag, Berlin, Heidelberg, pp. 519–522, doi:10.1.1.67.5472. Available at `http://portal.acm.org/citation.cfm/id=1763507.1763559`.

[MP07] M. A. Martins & D. Pigozzi (2007): *Behavioural reasoning for conditional equations*. *Mathematical Structures in Computer Science* 17(5), pp. 1075–1113, doi:10.1017/S0960129507006305.

[MSV84] T. S. E. Maibaum, M. R. Sadler & Paulo A. S. Veloso (1984): *Logical Specification and Implementation*. In: *Proceedings of the Fourth Conference on Foundations of Software Technology and Theoretical Computer Science*, Springer-Verlag, London, UK, pp. 13–30, doi:10.1007/3-540-13883-8-62.

[MVS85] T. S. E. Maibaum, P. A. S. Veloso & M. R. Sadler (1985): *A theory of abstract data types for program development: bridging the gap?* In: *Proceedings of the International Joint Conference on Theory and Practice of Software Development (TAPSOFT) on Formal Methods and Software*, Springer-Verlag, New York, NY, USA, pp. 214–230, doi:10.1007/3-540-15199-0_14. Available at `http://portal.acm.org/citation.cfm/id=22263.22277`.

[Roş00] G. Roşu (2000): *Hidden Logic*. Ph.D. thesis, University of California, San Diego.

[ST88a] D. Sannella & A. Tarlecki (1988): *Specifications in an arbitrary institution*. *Inform. and Comput.* 76, pp. 165–210, doi:10.1.1.144.2669.

[ST88b] D. Sannella & A. Tarlecki (1988): *Towards Formal Development of Programs from Algebraic Specifications: Implementations Revisited*. *Acta Informatica* (25), pp. 233–281, doi:10.1.1.17.6346.

[Tar95] A. Tarlecki (1995): *Moving Between Logical Systems*. In M. Haveraaen, O.J. Dahl & O. Owe, editors: *11th Workshop on Specification of Abstract Data Types, ADT?95*, Springer Lecture Notes in Computer Science (1130), pp. 478–502, doi:10.1.1.49.9260.

[Vou02] G. Voutsadakis (2002): *Categorical Abstract Algebraic Logic: Algebraizable Institutions*. *Applied Categorical Structures* 10, pp. 531–568, doi:10.1023/A:1020990419514.

[Vou03] G. Voutsadakis (2003): *Categorical Abstract Algebraic Logic: Equivalent Institutions*. *Studia Logica* 74, pp. 275–311, doi:10.1023/A:1024682108396.

[Vou05] G. Voutsadakis (2005): *Categorical Abstract Algebraic Logic: Models of π-Institutions*. *Notre Dame Journal of Formal Logic* 46(4), pp. 439–460, doi:10.1023/A:1020990419514.

[Wój88] R. Wójcicki (1988): *Theory of logical calculi. Basic theory of consequence operations.* Synthese Library, 199. Dordrecht etc.: Kluwer Academic Publishers.